37[11-02, 11Y05, 11Y11, 11Y16, 11Y35, 11Y40]—*Prime numbers and computer methods for factorization*, 2nd ed., by Hans Riesel, Progress in Mathematics, Vol. 126, Birkhäuser, Boston, 1994, xvi+464 pp., 24 cm, $69.50

The first edition was revised earlier [1]. Although both editions have the same number of pages, much new material has been placed in the second edition. Hardly any text from the first edition has been omitted from the second edition. The size has been maintained by replacing some tables by shorter ones and by using a smaller point size.

The long first-edition Chapter 5 on factorization has been split into two chapters in the second edition: "Classical Methods of Factorization" and "Modern Factorization Methods". Most of the new material appears in the second of these new chapters. There are new sections on the multiple-polynomial quadratic sieve, the elliptic curve method and the number field sieve (special and general). A lot of the background material for the book has been relegated to the eleven appendices. The second edition has new appendices on elliptic curves and higher algebraic number fields. With this new material, the second edition is an excellent introduction to all of the best-known factoring algorithms. The only omission I noticed was the FFT versions of the second steps of Pollard's $p-1$ method and the elliptic curve method.

The chapter on recognition of primes in the second edition treats elliptic curve primality proving, namely the tests of Goldwasser-Kilian and Atkin-Morain. Other new items reported in the second edition include: four new Mersenne primes 2^p-1, with $p = 110503, 216091, 756839$ and 859433; a new largest known twin prime pair $1692923232 \cdot 10^{4020} \pm 1$ found in 1993 by H. Dubner; some new first occurrences of large prime gaps and Jaeschke's new primality test for small numbers using strong pseudoprimes. It is reported that the Fermat number F_{22} is now known to be composite by Pepin's test. There is a section on Chebyshev's function $\theta(x)$. The first edition had tables of factors of $a^n \pm b^n$ for $1 \le b < a \le 10, \gcd(a,b) = 1$. The factor tables for $2^n \pm 1$ and $10^n \pm 1$ are retained in the second edition, but the other factor tables are replaced by tables of known factors of the generalized Fermat numbers $a^{2^n} + b^{2^n}$ for $a = 3, 4, 5, 6$, and $1 \le b < a$, $\gcd(a,b) = 1$, and also of $10^{2^n} + 1$ and $12^{2^n} + 1$. The table of Lucas' formulas for cyclotomic polynomials has been lengthened from degree 120 to 180, with its new coefficients contributed by Richard Brent. Many new references have been included.

Like the first edition, this clearly written text on factoring and prime testing will be welcomed by both novices and experts in the field.

References

1. S. S. Wagstaff, Jr., Review **3**, Math. Comp. **48** (1987), 439–440.

S. S. Wagstaff, Jr.
Department of Computer Sciences
Purdue University
West Lafayette, IN 47907